

Section	Administrative Procedure Number
Safety Procedures	RCJTC AP.03.10
Administrative Procedure Title	
Surveillance Procedure	
Date	Revised
December 21, 2013	October 5, 2016

Definitions

Personal Information: *The Municipal Freedom of Information and Protection of Privacy Act* defines personal information as being recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual’s race, colour, national or ethnic origin, gender, and age. Therefore, a simple image on a surveillance system that is clear enough to identify a person, or the activities in which he or she is engaged, will be classified as “personal information”.

Record: A record is defined to mean any information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record and any record that is capable of being produced from a machine-readable record.

Surveillance System: This refers to a physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic recording, observing or monitoring of individuals in school buildings, on school premises and buses. A surveillance system may also include audio devices, thermal imaging technology or any other component associated with recording the image of an individual.

Reception Equipment: Reception equipment is the equipment or device used to receive or record the personal information collected through a surveillance system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

Storage Device: A storage device is a videotape, computer disk, CD-ROM, computer chip, or other device used to store the recorded data or visual, audio or other images captured by a surveillance system.

Public Area: A public area is any location where students, staff and/or authorized visitors will have a reduced expectation of privacy. Such areas may include, but are not limited to school purpose vehicles, hallways, entrances, school grounds, assembly areas, stairways, general offices, meeting rooms, cafeterias and/or storage areas.

...Providing safe, efficient, effective transportation to our students

Any agreement between the RCJTC and the transportation operators shall state that the records created while delivering a surveillance program are under the RCJTC's control and are subject to the *Municipal Freedom of Information and Protection of Privacy Act*.

The RCJTC shall:

1. ensure that the records created while delivering a surveillance program are the sole proprietor of the records and as such are under the RCJTC's control and are subject to the *Municipal Freedom of Information and Protection of Privacy Act*;
2. provide training to transportation operators on the correct and lawful use of surveillance systems;
3. audit for compliance;
4. inform parents/guardians that a surveillance system may be used on vehicles;
5. be solely responsible to obtain information from the surveillance;
6. ensure that the use of a surveillance system relates to its intended use and no other purpose; and
7. ensure that the established procedures for the use of surveillance systems are respected.

The transportation operators shall:

1. be responsible for the proper and legal operation and maintenance of the surveillance equipment as authorized by the Renfrew County Joint Transportation Consortium; and
2. ensure that a sign is prominently displayed at the front of the vehicle to inform persons that surveillance is, or may be, in operation.

Access, Use, Disclosure, Retention, and Disposal of Surveillance Records

1. Access to surveillance records from vehicle cameras is controlled by the RCJTC designate.
2. Each transportation operator will designate one person who will have a key to extract the surveillance records.
3. The surveillance records can only be delivered to the RCJTC's designate.
4. Storage devices will be dated and labeled with a unique, sequential number and will be maintained in a secure location.
5. Logs will be kept of all instances of access and use of recorded material so as to provide for a proper audit trail.
6. Individuals whose information has been collected by a surveillance system have the right of access under the *Municipal Freedom of Information and Protection of Privacy Act*, unless an exemption applies under section 38. An example of an exemption would be where disclosure would constitute an unjustified invasion of another individual's privacy. Access to one's personal information would depend on:
 - a) if all third parties (i.e. those whose images appear on the record) give permission for the record to be viewed; or
 - b) whether it could reasonably be severed from the record, e.g. digitally "blacking out" the images of other individuals whose images appear on the record (storage device).

7. Any inadvertent disclosures of personal information or breaches of the *Municipal Freedom of Information and Protection of Privacy Act* or other relevant statutes shall be reported to the RCJTC and the respective member board's Freedom of Information and Records Management contact.
8. Transportation operators shall review and comply with this procedure and the *Acts* in performing their duties and functions relative to the operation of a recorded surveillance system. If a transportation operator fails to comply with the RCJTC/Board's policy or provisions of MFIPPA, it will be considered breach of contract leading to penalties up to and including contract termination.
9. Storage devices are set to record activity electronically to the limit of the memory in the device installed. Once the memory is full, the system will automatically overwrite the oldest data. Surveillance records must be erased after thirty (30) days. Records will be maintained in accordance with the *Municipal Freedom of Information and Protection of Privacy Act*.
10. The content of a storage device may be used to provide evidence to cause student discipline, e.g. suspension or expulsion. A storage device can be viewed by a student and his/her parent/guardian if:
 - a) all third parties (i.e. those whose images appear on the record) give permission for the record to be viewed; or
 - b) the images of other individuals who appear on the record (storage device) are severed from the record, e.g. digitally "blacked out".
11. When recorded activity is required in an investigation of student behavior or a student safety issue or in the investigation of other intruders or persons breaking the law, it will be transferred to an alternative storage device. Such storage devices used to assist in resolving transportation or public safety issues or law enforcement will be maintained in a locked, secured area by RCJTC for a one (1) year period from the date of resolution of the incident. Should it be necessary to release a storage device to police authorities, a Surveillance Recorded Material Release Form must be completed.
12. Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include shredding, burning, or magnetically deleting the personal information. A Storage Device Disposal Record is to be completed.

Related RCJTC Policy

P.03 *Safety Policy*

Related RCJTC Procedures

Related RCJTC Forms

F.03.10.1 *Surveillance Access Log Sheet*
 F.03.10.2 *Surveillance Recorded Material Release Form*
 F.03.10.3 *Storage Device Disposal Record*
 F.03.10.4 *Surveillance Sign for Vehicle*
 F.03.10.5 *Surveillance Notification to Parents*